Usefulness of privacypass APIs on the Web

Steven Valdez

IETF 119 - PRIVACYPASS - 2024-03

Agenda

- Related APIs
- Attester/Issuer Ecosystem
- Future Work

Related APIs

- Private Access Tokens
  - Split attester/issuer instantiation of privacypass.
  - Rate-limited tokens.
- Private State Tokens
  - Joint attester/issuer model
  - Based on VOPRF-style tokens and format.
  - Does not implement privacypass authentication scheme.
  - Previously had a private metadata variant.
- Chrome IP Protection
  - Using privacypass style RSA tokens with metadata (see metadata discussion).

Attester/Issuer Ecosystem

- Single/Fixed-Set Attester/Issuers
  - Properties of the attester are well-known.
  - Limitations on amount of data based on the limited number of parties.
  - Private Access Tokens
  - IP Protection Tokens
  - Well understood meanings for tokens.
- Arbitrary Attesters/Issuers
  - Differing levels of trust in the parties in the ecosystem.
  - Mitigations at issuance/redemption time to avoid many issuers being used in the same context.
  - Private State Tokens
  - Fuzzier meanings for tokens.

Challenges

- Mitigations to limit redemptions across multiple issuers can cause issuer pinning.
  - Mechanisms to limit cross-issuer collusion without permanent pinning of issuers to each redemption context?
- Binding redemption to a particular context.
  - The challenge can help mitigate this, but in cases where there are lower traffic issuers, the timing correlation between an issuance and redemption event introduces additional side channels.

Open Questions/Future Work

- More nuanced analysis of how different issuers interact with each other in an ecosystem.
  - How to measure the privacy impact and how to support rotation.
- Technical mechanisms for classifying tokens/issuers and how they are used.
  - Governance vs centralization discussion.
- Changing meaning over time can result in additional complexity.
- How different issuer ecosystems interact.